IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

Privacy Threats in Facial Recognition-Based Identity Verification

Latika Kharb and Deepak Chahal
Professor, Jagan Institute of Management Studies, Rohini, Delhi, India
latika.kharb@jimsindia.org

Abstract: *Facial recognition technology has gained significant prominence in identity verification systems, providing convenience and security in various domains. However, the widespread adoption of this technology also raises significant concerns regarding privacy threats. This paper presents a comprehensive privacy threat model specifically designed for identity verification based on facial recognition. The model encompasses potential adversary objectives, such as unauthorized access, identity theft, and profiling, and identifies specific privacy threats, including unauthorized data access, biometric data misuse, tracking and surveillance, re-identification attacks, discrimination and bias, and data retention and sharing. To mitigate these threats, the paper proposes several mitigation measures, such as informed consent, transparent data handling, secure data storage and transmission, minimization of data collection, regular audits and assessments, and ethical considerations. By providing a holistic view of privacy threats in facial recognition-based identity verification, this model aims to guide researchers, practitioners, and policymakers in developing and implementing effective privacy protection mechanisms in this rapidly evolving technological landscape.*

Keywords: Facial recognition

I. INTRODUCTION

Facial recognition technology is a biometric technology that uses computer algorithms to identify and verify individuals based on their facial features. It analyzes unique patterns, such as the arrangement of eyes, nose, mouth, and other facial characteristics, to create a mathematical representation, also known as a facial template or faceprint. This technology can be applied in various contexts, including identity verification, surveillance systems, access control, and personalization.

The process of facial recognition typically involves the following steps:

Face detection: The technology detects and locates faces within an image or video frame, often utilizing advanced algorithms to differentiate faces from other objects.

Face alignment: Facial landmarks, such as the position of eyes, nose, and mouth, are identified and aligned to establish a standardized reference for accurate analysis.

Feature extraction: Key facial features are extracted from the aligned face image, such as the shape of the face, texture, and specific details like the distance between eyes or the curvature of the lips.

Face matching: The extracted facial features are compared against previously stored templates or a database of known faces. This matching process involves complex algorithms that calculate the similarity or dissimilarity between facial templates to determine potential matches.

Identification or verification: In identification mode, the system attempts to determine the identity of an individual by comparing their face to a large database of enrolled faces. In verification mode, the system verifies if the presented face matches a specific individual's face already known and enrolled in the system.

Facial recognition technology has evolved significantly over the years, driven by advancements in machine learning, computer vision, and deep neural networks. It offers benefits such as improved efficiency, enhanced security, and personalized experiences. However, it also raises concerns about privacy, surveillance, and potential misuse of biometric data, highlighting the need for responsible and ethical deployment and regulation of this technology.In the context of identity verification systems utilizing facial recognition technology, it is crucial to understand the potential

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

privacy threats that individuals may encounter. While facial recognition can provide convenience and security in various applications, it also poses significant risks to personal privacy. This threat model aims to outline potential privacy concerns associated with facial recognition-based identity verification systems.

II. PRIVACY THREATS INVOLVED IN FACIAL RECOGNITION

- Unauthorized data access: Adversaries may attempt to breach the facial recognition system's database or intercept data during transmission, potentially exposing individuals' facial images, biometric data, or personal information.
- Biometric data misuse: Facial recognition systems rely on capturing and storing individuals' biometric data. Adversaries might exploit this data to impersonate individuals or perform malicious actions, such as creating synthetic faces for bypassing the system.
- Tracking and surveillance: Facial recognition systems integrated into surveillance networks can enable continuous tracking and monitoring of individuals, raising concerns about mass surveillance and loss of anonymity.
- Re-identification attacks: Adversaries could use facial recognition data to re-identify individuals in other contexts or cross-reference it with other data sources, leading to potential privacy breaches.
- Discrimination and bias: Facial recognition systems may exhibit biases, leading to inaccurate identification or differential treatment based on factors like race, gender, or age, thereby posing privacy risks and exacerbating social inequalities.
- Data retention and sharing: Organizations implementing facial recognition systems might retain individuals' facial images or biometric data beyond the necessary verification period, which can increase the likelihood of data breaches or unauthorized access.

III. REQUIREMENT OF MITIGATION MEASURES TO OVERCOME PRIVACY THREATS

To address these privacy threats, several mitigation measures can be implemented:

- Informed consent: Individuals should be provided with clear and detailed information about the purpose, scope, and potential risks associated with facial recognition-based identity verification systems. They should have the right to provide informed consent before their data is collected or processed.
- Transparent data handling: Organizations should adopt transparent practices for data collection, storage, and sharing. They should clearly outline their data retention policies and ensure compliance with relevant privacy regulations.
- Secure data storage and transmission: Robust security measures, such as encryption, access controls, and secure protocols, should be implemented to protect facial images, biometric data, and personal information from unauthorized access or interception.
- Minimization of data collection: Organizations should limit the collection and storage of facial images and biometric data to the minimum necessary for identity verification purposes, reducing the risk of data breaches.
- Regular audits and assessments: Independent audits and assessments should be conducted to evaluate the facial recognition system's accuracy, fairness, and compliance with privacy standards. This helps identify and rectify potential biases or vulnerabilities.
- Biometric data protection: Organizations should implement strong safeguards to protect stored biometric data, such as secure hashing and encryption, ensuring that it cannot be reverse-engineered or misused.
- Regular system updates: Facial recognition systems should receive regular updates to address vulnerabilities and improve accuracy. This includes staying up to date with advancements in facial recognition technology and algorithmic improvements.
- Ethical considerations: Organizations should adopt ethical guidelines that address concerns related to bias, discrimination, and privacy. This includes testing facial recognition systems for fairness across various demographic groups and taking steps to mitigate bias.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

IV. RESULTS AND CONCLUSION

In conclusion, this paper has explored the privacy threats inherent in facial recognition-based identity verification systems. The widespread adoption of facial recognition technology brings significant convenience and security benefits but also raises concerns about individual privacy. The identified privacy threats encompass unauthorized data access, biometric data misuse, tracking and surveillance, re-identification attacks, discrimination and bias, and data retention and sharing.

To address these threats, a comprehensive understanding of the targeted systems and their common aspects is crucial. The proposed taxonomy serves as a controlled vocabulary, enabling the description and classification of different use cases found in the literature. This taxonomy facilitates practitioners' comprehension of the systems' processes, assets, involved agents, and information flows.

Furthermore, the identified common aspects across application domains provide a foundation for generic privacy threat modelling applicable to all these domains. By employing robust privacy protection measures, such as informed consent, transparent data handling, secure storage, and regular audits, organizations can mitigate privacy threats and uphold individuals' privacy rights.

It is essential for practitioners, researchers, and policymakers to consider these privacy threats and adopt responsible practices when implementing facial recognition-based identity verification systems. By striking a balance between the benefits of facial recognition technology and protecting individuals' privacy, we can ensure the ethical and responsible use of this technology in an increasingly digitized world. Future research should continue to explore and address evolving privacy concerns as facial recognition technology advances.

REFERENCES

[1] Li, Y., Jain, A. K., & Li, S. Z. (2011). Handbook of Face Recognition. Springer Science & Business Media.

[2] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

[3] Brömme, A., Busch, C., & Rathgeb, C. (Eds.). (2018). Handbook of Biometric Anti-Spoofing: Presentation Attack Detection. Springer International Publishing.

[4] Bolle, R. M., Jain, A. K., &Pankanti, S. (Eds.). (2005). Biometrics: Personal Identification in Networked Society. Springer Science & Business Media.

[5] Kharb L, Rai B, Tomar P, "New Vision of Computer Forensic Science: Need of CyberCrime Law", The Internet Journal of Law, Healthcare and Ethics, 2007. Volume 4, Number 2. ISSN: 1528-8250.

[6] Kharb, L. A Perspective View on Commercialization of Cognitive Computing. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering, IEEE.

[7] Kharb, L. The Hackers: Shadow Brokers, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017

[8] Kharb L, IBM Blue mix: Future development with open cloud architecture, International Journal of Information Communication and Computing Technology, Vol. 3(2), 2015, pp. 165-168.

[9] Chahal D, Kharb L,Data security in Cloud Computing, International Journal of Engineering and Science Invention, Vol. 6 (12), 2017, pp. 31-36.

[10] Sachdeva, G ,Verma, R , Chahal D, Kharb L, Photovoltaic Cells Embedded Road for Electric Vehicle Charging (April 4, 2020). Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020, Available at SSRN: https://ssrn.com/abstract=3568406 or http://dx.doi.org/10.2139/ssrn.3568406.

[11] Kharb, L., Chahal, D., Vagisha (2021). Smart Mobility: Understanding Handheld Device Adoption. In: Hura,G., Singh, A., Siong Hoe, L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering, vol 668. Springer, Singapore. https://doi.org/10.1007/978-981-15-5341-7_2

[12] Kharb L, Singh P (2021) Role of machine learning in modern education and teaching. In: Impact of AI technologies on teaching, learning, and research in higher education. IGI Global, pp 99–123

[13] Ang, L. M., Seng, K. P., & Zhang, Y. (2019). Biometrics and privacy: A review. Journal of Biomedical Informatics, 95, 103206.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

[14] Solanki, R., & Chatterjee, S. (2018). Facial recognition technology: Privacy and ethical concerns. In Proceedings of the 2018 International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 1-5). IEEE.
[15] Cavoukian, A., & Castro, D. (2019). Privacy by design: Essential for organizational accountability and strong business practices. IEEE Security & Privacy, 17(3), 85-89.
[16] Colclough, N., & Millard, C. (2019). Regulating facial recognition technology in 2019: An international comparison. Computer Law & Security Review, 35(6), 100-116.
[17] Mayer-Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt.